ALPHABAY EXIT, HANSA-DOWN: DREAM ON?

EXAMINING THE EFFECTS OF OPERATION BAYONET ON DREAM MARKET

Rolf van Wegberg
Thijmen Verburgh
Jorrit van den Berg
Mark van Staalduinen

TNO innovation for life

RECENTLY, DURING OPERATION BAYONET TWO LEADING UNDERGROUND MARKETS ON THE DARK WEB TOOK CENTER STAGE IN A JOINT POLICING EFFORT OF THE FEDERAL BUREAU OF INVESTIGATION (FBI) AND THE NATIONAL HIGH TECH CRIME AND DARK WEB UNIT OF THE DUTCH POLICE. IN A COORDINATED SWEEP, THE FBI SUCCEEDED IN THE TAKEOVER AND SUBSEQUENTLY TAKE DOWN OF ALPHABAY, WHILE THE DUTCH POLICE TOOK OVER, RAN AND SHUT DOWN HANSA MARKET. BY PLANNING THESE ACTIONS SEQUENTIALLY, THE POLICE AGENCIES EXPECTED CRIMINALS ACTIVE ON ALPHABAY TO MAKE THEIR WAY TO HANSA MARKET – WHICH AT THAT MOMENT WAS OPERATED BY THE DUTCH POLICE. THIS PUT THE POLICE AGENCIES IN A PERFECT POSITION TO NOT ONLY DISRUPT THE ECOSYSTEM, BUT ALSO TO COLLECT VALUABLE DATA ON THOUSANDS OF USERS.

With regard to the effects of operation Bayonet, three questions stand out:

1) How did the police carry out this innovative intervention?
2) Did it work? and
3) Was this all legal?

Because more details are still coming to light about the operation itself, and ultimately the question on the legality of the operation will be put before the courts, we will focus on the second question: did it work?

IN ONLY EIGHT MONTHS' TIME DREAM MARKET NEARLY DOUBLED ITS USER BASE TO ALMOST 16000 USERS

Leveraging on the insights of previous take-downs - like Silk Road 1.0 and 2.0 cases - we know that a typical result of a take-down is that users 'migrate' to other markets and carry on with their illegal business operations. Researchers from Carnegie Melon University[I] (CMU) studied the overall trade-volume on other underground markets after both Silk Road take-downs. Although the trade-volumes changed, they increased instead of decreased. Noteworthy are also the findings of sociologist Ladegaard,[II] who linked the media-attention to both take-downs to this increased sales-volume. In conclusion, we can say that take-downs often result in a so-called 'waterbed-effect' or a game of 'Whack-a-Mole'. An intervention aimed at one part of the underground market ecosystem, results in the growth of another part, without reaching the objective of the intervention: lowering crime across the ecosystem. Police agencies seem determined to break with this 'tradition' and have changed their method of intervention to tackle precisely this unwanted side-effect. So, did it work?

To observe the first effects of Operation Bayonet, we studied the user-base on another underground market: Dream Market. This Market was established at the end of 2013 and has grown steadily ever since, making it a perfect market for our analysis. At the beginning of this year we recorded around 8,500 Dream Market users. Up until July 2017 Dream Market had about 20 new users per day. That changed significantly from July onwards, when Dream Market began acquiring more than 60 new users per day. On some days as many as 180 new users registered (Figure 1).

In a period of just eight months, Dream Market nearly doubled its user base to almost 16,000 users (Figure 2). Looking at the timing, we can state that the steep influx of users in July was probably the direct result of Operation Bayonet – in which AlphaBay went down on July 4th and Hansa Market was shut down on July 20th – making Dream Market the leading underground market.

NEW USERS PER DAY ON DREAM MARKET IN 2017

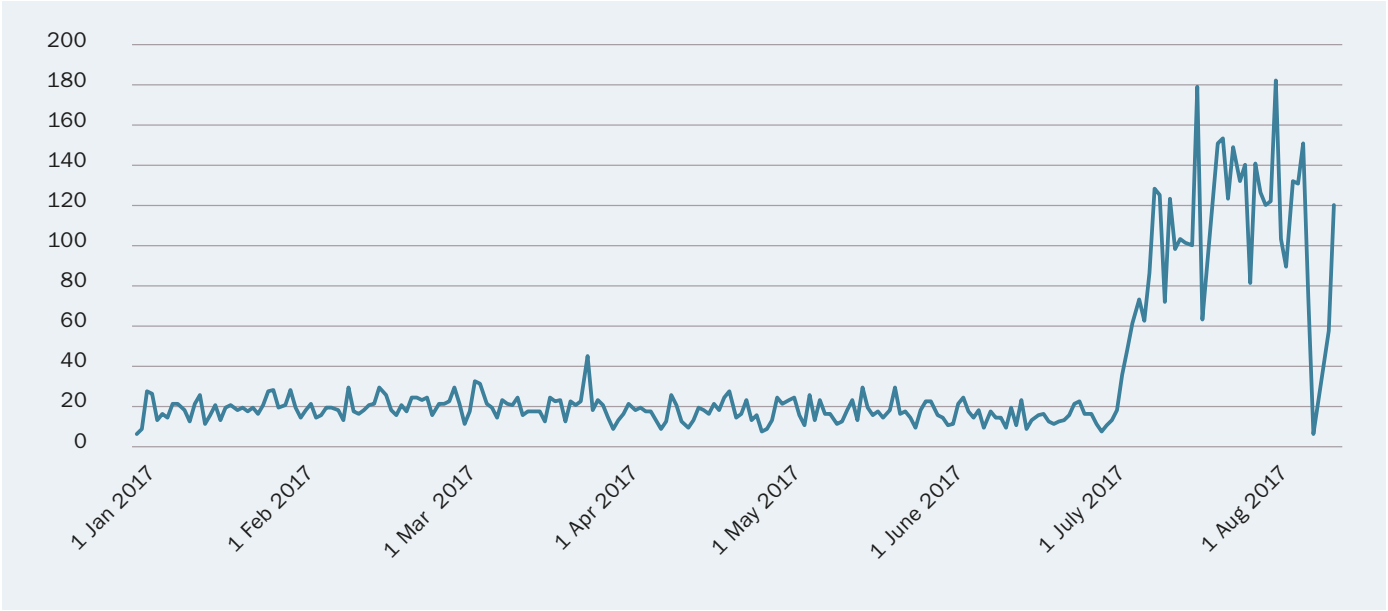

Figure 1

USERS ON DREAM MARKET IN 2017

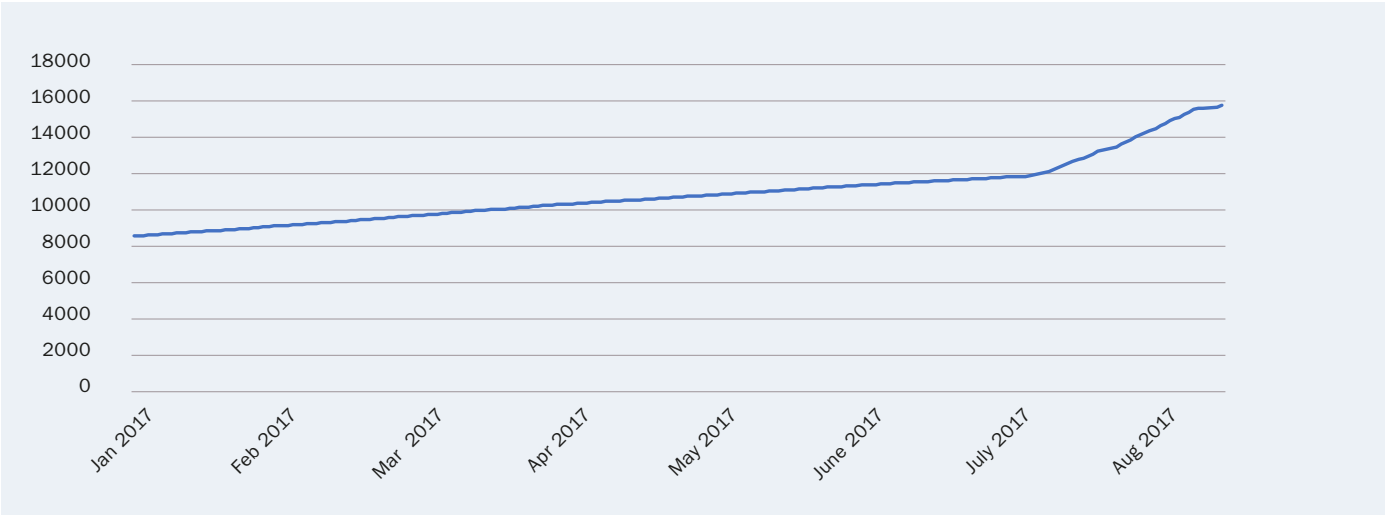

Figure 2

However, looking at the number of users of AlphaBay – where, according the US Attorney-General Sessions over 40,000 vendors were selling to more than 200,000 buyers[III] - and Hansa Market prior to their takedown, certainly not all users 'migrated' to Dream Market. Nevertheless, the increase of users is consistent with earlier take-down effects. To properly assess the detailed effects of Operation Bayonet, we looked specifically at the newly registered vendors on Dream Market (n=195), their background and whether or not they changed their behaviour after the police operation.

After obtaining the usernames of the 195 vendors that registered on Dream Market between July 1st and August 15th, we used Grams (a specific Dark Market search engine) to map specific characteristics of these vendors. Utilizing Grams, we determined where the vendor 'migrated' from: AlphaBay, Hansa Market, both, or whether they migrated to Dream Market from another market. We also determined if the username of the vendor was used before on underground markets, making this vendor to the regular buyer look like a 'new' vendor without any reputation. Next, we identified vendors that changed usernames, but stuck to their PGP-key, or that stuck to their username but changed PGP-keys.

Figure 3 shows the breakdown of newly registered vendors on Dream Market. There are two striking facts: 1) whilst many vendors migrated from AlphaBay to Dream Market, almost none did so from Hansa Market to Dream Market; 2) unexpectedly, many of the newly registered vendors were completely 'new' and without any reputation or track-record.

When we look at the 'migrated' vendors, so the 117 users that were active on AlphaBay, Hansa or even both, the question arises: Did they put any effort into evasive measures after both take-downs?

BREAKDOWN OF NEWLY REGISTERED VENDORS ON DREAM MARKET (N=195)

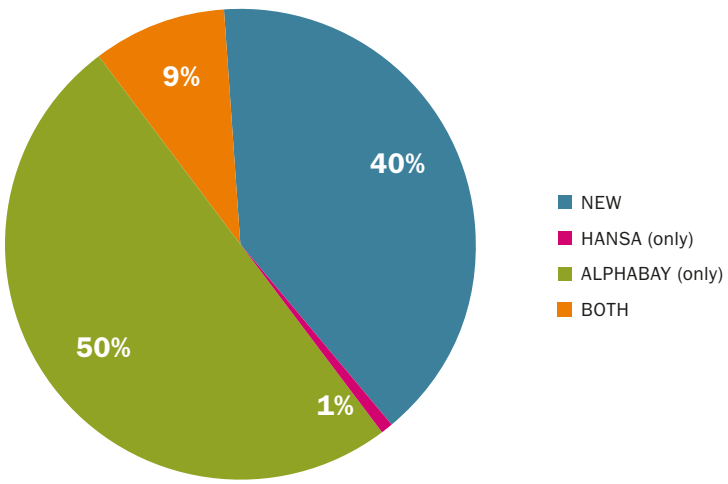

Figure 3

BREAKDOWN OF EVASIVE STRATEGIES OF MIGRATED VENDORS TO DREAM MARKET (N=117)

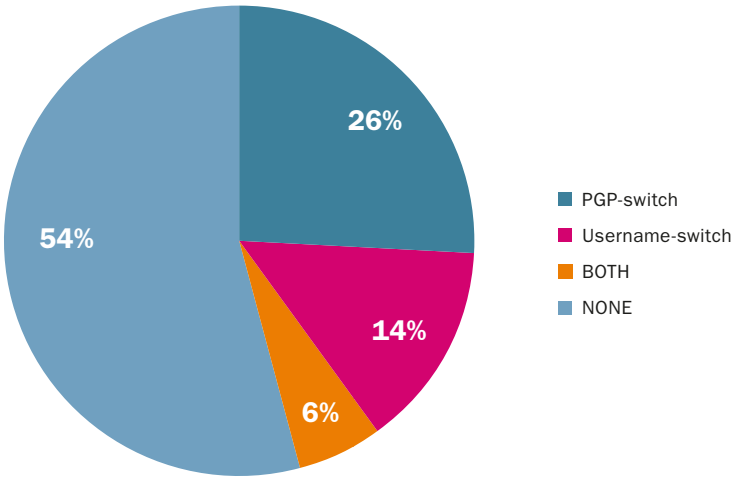

Figure 4

26% OF USERS CHANGED THEIR PGP-KEYS AND 14% CHANGED THEIR USERNAMES

Figure 4 shows that more than half of the 'migrated' users did not take any noticeable evasive measures. However, we can see that 26% of users changed their PGP-keys and 14% changed their usernames. As a username and PGP-key are valuable assets in an anonymized setting – like underground markets - users do not change PGP-keys or usernames unless they really have to. The number of evasive measures, combined with the number of 'new' vendors are a strong indicator that this police intervention has achieved more than might be apparent at first sight, when looking more closely at the influx of users to Dream Market. It hints towards a panicking community of users trying to start over, whether with a new username, a new PGP-key or a more thorough start over altogether.

We can assess this scenario even further by looking at these elements of migration pattern and evasion measures longitudinally. By doing so, we can see if the behaviour of these vendors after the AlphaBay take-down – where no police infiltration took place – differs from the Hansa takedown – where the police infiltrated, disabled encryption on personal messages and could see everything being said and done for three weeks without arising any suspicion.

BREAKDOWN OF EVASIVE STRATEGIES OF MIGRATED VENDORS TO DREAM MARKET (N=117)

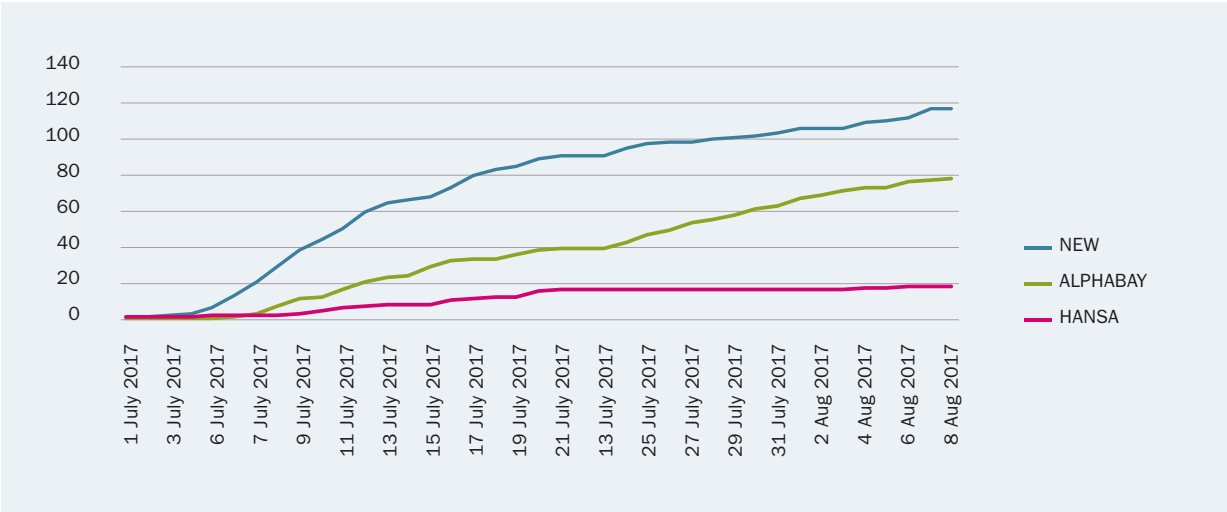

Figure 5

CUMULATIVE NUMBER OF EVASIVE MEASURES BY NEWLY REGISTERED VENDORS ON DREAM MARKET ON DATE (N=47)

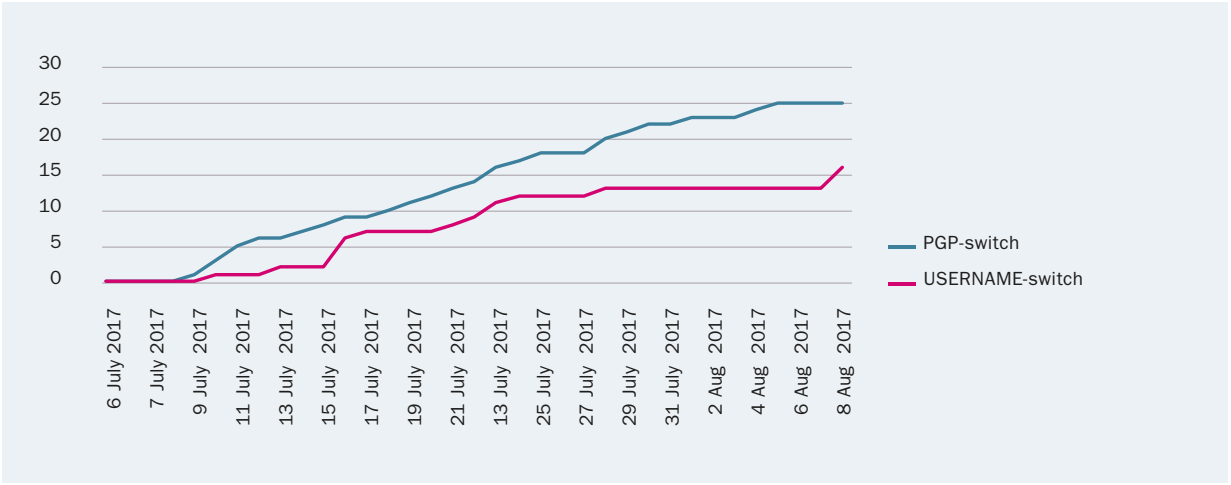

Figure 6

Figure 5 shows the cumulative number of newly registered vendors during our period of analysis in July and August. Noticeably the influx of AlphaBay 'migrants' stays relatively stable during the time-period described. However, the number of 'new' vendors increases, whilst the number of Hansa migrants stagnates at the same time: immediately following the Hansa Market take-down. This is accompanied by a complete standstill in newly registering vendors on 22nd and 23rd of July. All this builds to a picture of a panicking community right after the Hansa take-down.

This scenario is further supported by the evasive measures (Figure 6). Right after the Hansa takedown, the username-switch stagnates. In turn, vendors apparently take a more drastic measure: starting over.

In summary, we see the first signs of game-changing police intervention. Compared to both the Silk Road take-downs, or even the AlphaBay takedown, the Hansa Market shut down stands out in a positive way. Sharply contrasting the waterbed-effect of previous law enforcement efforts on underground market, users do not just move along after the Hansa Market shutdown. Few simply 'migrate'; whilst some take precautions like changing their username and/or PGP-key, there are many that start over completely. This may sound like a minor detail in such a complicated intervention, but the opposite is the case.

When a vendor 'starts over' they lose their track-record, reputation and clientele. Like a Michelin star restaurant changing its name, location and phone-number: their business will implode.

We have to see if the effects of this innovative intervention hold out in the long run, but for now the effects are remarkable in the light of earlier Dark Web-interventions.

[I] Soska & Christin (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, *Proceedings of the 24th USENIX Security Symposium*, https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf

[II] Ladegaard (2017). We Know Where You Are, What You Are Doing and We Will Catch You: Testing Deterrence Theory in Digital Drug Markets, *The British Journal of Criminology*, https://doi.org/10.1093/bjc/azx035

[III] https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

TNO.NL

DARK WEB SOLUTIONS

TNO
Rolf van Wegberg
Cybercrime researcher
E rolf.vanwegberg@tno.nl

17-9099 aug 2017